

Listing of Claims

1-45. (canceled)

46. (previously presented) A device, comprising:

a classification module in the device that determines security association information associated with each data packet in a plurality of data packets associated with a data flow between a source and destination, wherein the classification module is configured to determine the security association information for the plurality of data packets simultaneously;

a plurality of security processing engines in the device, coupled to the classification module, each of the plurality of security processing engines configured to receive at least a portion of the security association information associated with a data packet in the plurality of data packets along with the corresponding data packet, wherein at least two of the plurality of security processing engines receive security association information for different packets,

wherein the classification module is configured to provide at least a portion of the security association information associated with the data packets to the plurality of security processing engines; and

wherein the plurality of security processing engines are configured to process the plurality of the data packets in the data flow in parallel.

47. (previously presented) The device of claim 46, further comprising a database in the device including security association information, wherein the database is local to the classification module.

48. (previously presented) The device of claim 47, wherein the database includes one or more entries, wherein each entry defines information associated with one security association.

49. (previously presented) The device of claim 48, wherein the database is located on the same chip as the classification module.

50. (previously presented) The device of claim 46, wherein the security association information includes a sequence number, an anti-replay window, and a lifetime of the security association.

51. (previously presented) The device of claim 50, wherein the security association information further includes an encapsulating security payload (ESP) encryption algorithm identifier and one or more ESP encryption keys.

52. (previously presented) The device of claim 51, wherein the security association information further includes an ESP authentication algorithm identifier and one or more ESP authentication keys.

53. (previously presented) The device of claim 50, wherein the security association information further includes an authentication header (AH) authentication algorithm identifier and one or more AH authentication keys.

54. (previously presented) The device of claim 50, wherein the security association information includes protocol mode information.

55. (previously presented) The device of claim 47, wherein the database is stored in memory.

56. (previously presented) The device of claim 55, wherein the memory is contact addressable memory (CAM).

57. (previously presented) The device of claim 55, wherein the memory is random access memory (RAM).

58. (previously presented) The device of claim 46, wherein the device is a router.

59. (previously presented) The device of claim 46, wherein the device is a firewall.

60. (previously presented) The device of claim 46, wherein the device is a network communication device.

61. (previously presented) The device of claim 46, wherein the device is a security gateway.

62. (previously presented) The device of claim 46, wherein the device is a server.

63. (previously presented) The device of claim 46, wherein the device is a network line card.

64. (previously presented) A method for classifying data packets during security processing in a device, comprising:

receiving, in the device, at least a portion of a header for each data packet in a plurality of data packets associated with a data flow between a source and destination;

simultaneously determining security association information associated with each data packet in the plurality of data packets in the data flow;

receiving at least a portion of the security association information associated with a data packet in the plurality of data packets along with the corresponding data packet at each security processing engine in a plurality of security processing engines in the device, wherein at least two of the plurality of security processing engines receive security association information for different packets in the data flow; and

processing the plurality of data packets in the data flow in parallel.

65. (previously presented) The method of claim 64, wherein the step of determining security association information comprises:

accessing a database in the device to determine security association information.

66. (previously presented) The method of claim 65, wherein the step of determining security association information further comprises:

using one or more selectors to identify a security association entry in the database.

67. (previously presented) The method of claim 66, wherein the one or more selectors include at least one of a destination IP address, a security protocol identifier, and a security parameter index.

68. (previously presented) The method of claim 66, wherein the one or more selectors include a destination IP address, a source IP address, and a transport layer protocol.

69. (previously presented) The method of claim 68, wherein the one or more selectors further include a source port and a destination port.

70. (previously presented) The method of claim 65, wherein the step of determining security association information further comprises:

if no security association information exists in the database associated with the packet, generating the security association information; and
storing the security association information in an entry in the database.